



The Complete Checklist for True SASE Platforms

Sponsored by US Signal and CATO Networks

Architecture

Security

Networking

Management



How to Spot Real and Fake SASE

The Secure Access Service Edge (SASE), introduced by Gartner in 2019, is a cloud-based architecture built to deliver networking and security capabilities to all locations, users, and devices — globally. Gartner positioned SASE as a transformational category that will change the way IT organizations deliver secure, optimized application access to their users. These capabilities include SD-WAN, Secure Web Gateway (SWG), Firewall as a Service (FWaaS), Zero Trust Network Access (ZTNA/SDP), Cloud Access Security Broker (CASB), and more.

Many vendors providing legacy networking and security solutions have jumped on the SASE bandwagon. However, if these vendors are true SASE providers, what is the innovation represented by the brand-new SASE category? The answer is that these SASE vendors focus on the actual capabilities, which have not changed, and ignore the architecture which has changed. In other words, SASE isn't redefining the capabilities themselves, but rather the way they are delivered, scaled, distributed, enhanced, and managed.

This architectural change, driven by the move to the cloud and a distributed workforce, is very difficult for vendors that are relying on legacy, pre-SASE architectures.

In the checklist below we highlight the attributes and capabilities of a true SASE architecture and explain why they are essential to the transformational power of SASE.

Architecture

1 Convergence

Convergence in the SASE context refers to a single pass engine that optimizes and secure network traffic. When a packet goes through the SASE single pass engine it is:

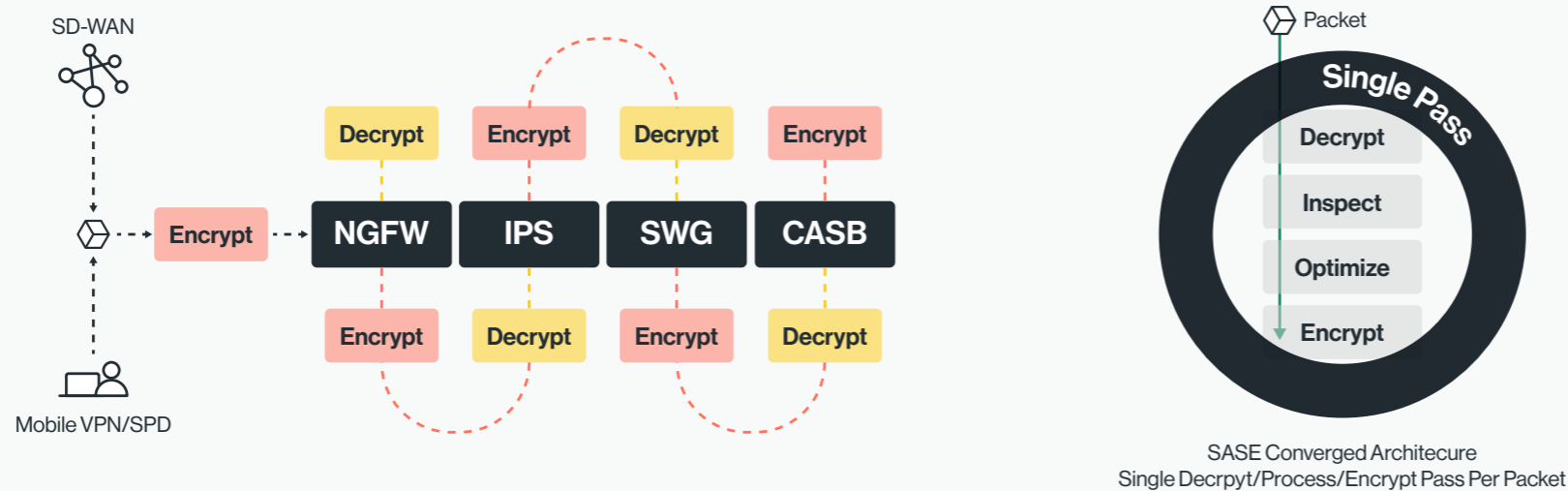
- Associated with a user identity and target application context
- Decrypted and inspected for threats, risks, and data sensitivity
- Prioritized for available network capacity, and
- Optimally routed to the destination

The single pass engine converges all these process requirements to eliminate the latency and overhead resulting from moving the packets through multiple products, decryption cycles, and policy engines.

Requirement

A true SASE platform uses a converged, single pass engine to optimize and secure all traffic regardless of source and destination.

Multi-pass vs. Single-pass Architecture



Architecture

2 | Cloud-based

SASE is a cloud-native and cloud-based service that is running the converged single pass engine. Some vendors argue that SASE can be delivered from an on-premises appliance, but this defeats the purpose and reasoning behind SASE. Placing the SASE single pass engine in the cloud, creates the following benefits:



Elasticity

The SASE provider can scale the capacity of the service without impacting the user environment. This eliminates the need to upgrade and replace edge appliances as traffic grows, new capabilities are introduced and traffic mix changes.



Extensibility

The SASE cloud service is “close” to all edges: locations, users, clouds, and applications. This is a key architectural advantage over appliances that “lock” these capabilities inside a specific edge location such as a datacenter or a branch. This problem was clearly demonstrated during the COVID-19 pandemic where expensive branch networking and security equipment was sitting idle with all users working from home.



Self-maintaining

The SASE cloud service software and hardware are fully maintained by the SASE provider. There is no need to patch individual boxes, a risky and time-consuming process.



Self-healing

High availability design is a complex activity. It requires IT to consider, plan, and deploy redundant infrastructure to address local, regional, and global outage scenarios. The SASE cloud service is designed and built with very deep resiliency and redundancy to ensure the service continues to operate under adverse conditions.

Requirement

A true SASE platform is built on a cloud-native, cloud-based service to leverage the elasticity, extensibility, and redundancy of the cloud.



Appliance

Location-bound

Capacity Constrained

High Maintenance

Complex HA

Different Models



SASE Cloud PoP

Location-independent

Elastic Capacity

Self-Maintaining

Self-Healing

Symmetrical

Architecture

3 Global

One of the architectural attributes of a SASE cloud service, is the ability to extend the service globally. The SASE provider deploys the single pass engine across multiple Points of Presence (PoPs) in different regions, so they are placed close to enterprise edges. This eliminates the need to build regional enterprise “hubs” needed to deliver advanced security and networking capabilities for regional offices and users. A truly global SASE service provides the following benefits:



High Coverage Density

The SASE PoPs should be placed within 25ms latency of every user and location to ensure optimal performance.



Flexible Coverage

The SASE provider must be able to deploy PoPs anywhere, and specifically beyond the typical footprint of cloud hyperscalers (i.e., countries like China, Latin America, Africa, etc.). DevOps and NetOps competencies are essential when deploying such PoPs, both physical and virtual.

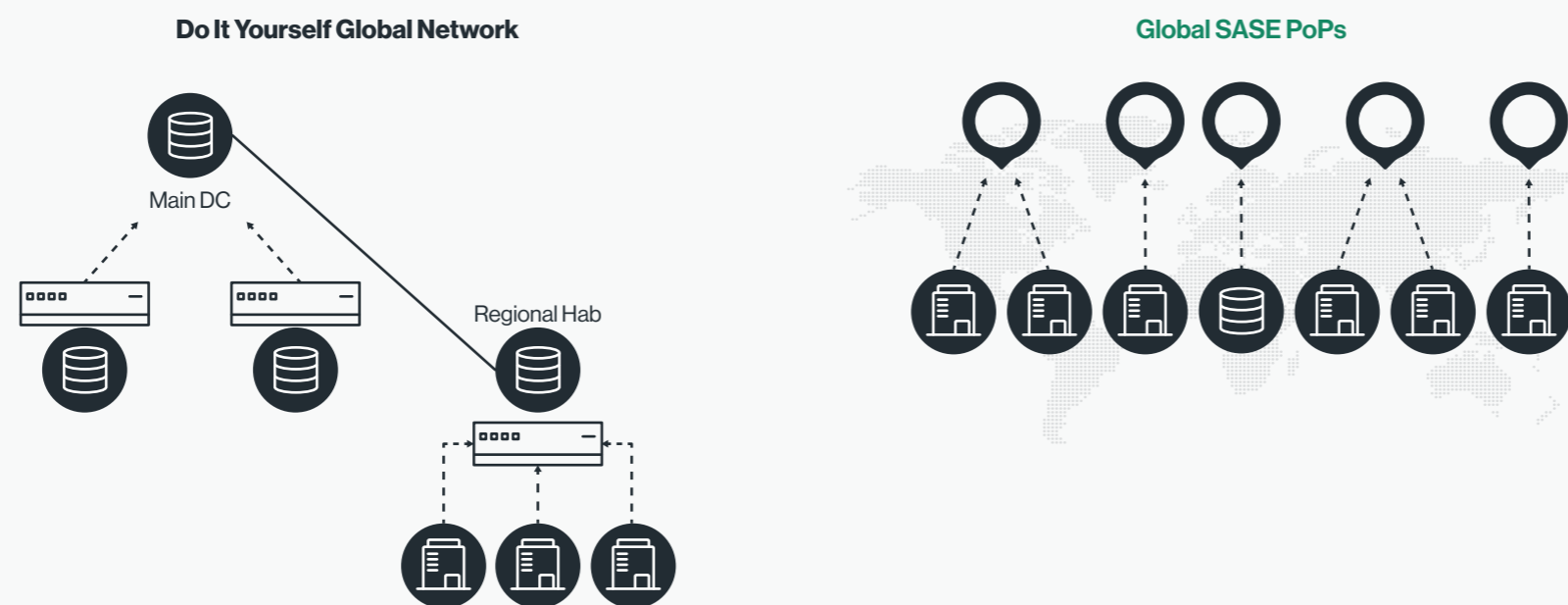


Maximized End-to-End Throughput to On-premises and Cloud apps

One of the challenges of global access to bandwidth intensive apps (i.e., files uploads/downloads) is the ability to maximize bandwidth end to end. The SASE software should include acceleration capabilities that will boost throughput when compared to good transports that aren't optimized (i.e., MPLS). Since apps can be located anywhere there is a need to deliver the optimization for both WAN and Internet traffic globally.

Requirement

A true SASE platform is globally distributed to enable high-performance access to applications, on-premises and in the cloud, from everywhere and by anyone.



Architecture

4 All Edges

True SASE architectures treat each edge resource equally. An edge can be a physical or cloud datacenter, a branch, a personal device, or an IOT device. All these edges require optimal and secure access to other resources within the enterprise, in the cloud, and on the Internet. The SASE service acts as a “cloud switchboard” that connects the edges on the one hand, and the destinations on the other hand, while accelerating and securing the traffic the flows back and forth. Connecting all edges to the SASE service has the following benefits:



Full Traffic Visibility and Control

The SASE service optimizes traffic from all edges to the Internet and the Cloud (northbound) as well as traffic between edges over the Wide Area Network (east-west). Therefore, a true SASE service provides predictable connectivity for all critical and loss sensitive applications wherever they reside (including voice, remote desktops, and business applications). This means a SASE service, at its core, must rely on a reliable global backbone that can optimize all these types of traffic.



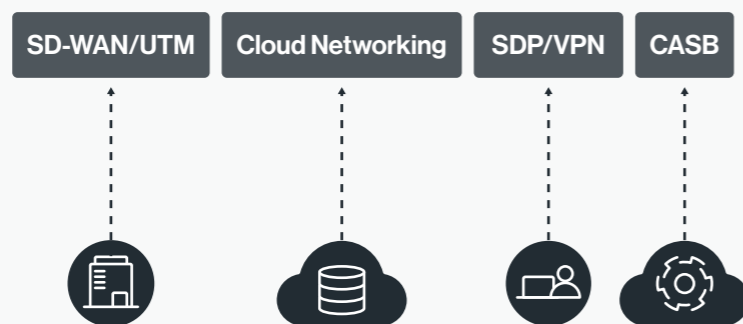
Seamless support for Cloud Migration and Work from Anywhere

Organizations that are gradually migrating to the cloud, will find this all-inclusive architecture valuable as an application or service may reside “on premises” (WAN access) today and migrate to a public SaaS platform (cloud access) tomorrow. The same is true for users that work from the office, on the road, and at home essentially switching edge connections as they move around.

Requirement

A true SASE platform is based on a cloud-first/thin client architecture designed to equally support all edges (locations, clouds, devices, users, applications) and provide all underlying security and optimization capabilities to all traffic from all edges to all applications.

Separate point solution per edge



Edge On Ramps into a SASE platform



Capabilities: Networking

The networking layer of SASE includes the connectors into the SASE cloud service (“the on ramps”) and the way SASE optimizes traffic within the cloud service itself (“the middle mile”).

Requirement

A true SASE platform uses a global private backbone that supports both WAN and cloud traffic to address the broadest set of use cases and enterprise requirements with a predictable and consistent connectivity from all users to all applications.

The SASE On-Ramps: Edge SD-WAN and Device Clients

Connectivity to the SASE cloud service is based on encrypted tunnels that originate from an edge (SD-WAN device, a SASE Client, IPsec capable device) to the nearest SASE PoP. At the PoP and within the service all SASE capabilities apply to all traffic from all edges.



SD-WAN Edge device

Establishes one or more tunnels to the Cato PoP. SD-WAN capabilities include active/active link management, dynamic path selection based on link behavior, application- and identity-aware QoS, and packet loss mitigation. The SD-WAN device primary function is to ensure traffic reaches the SASE PoP in the most efficient, resilient, and optimal way. The SD-WAN edge devices, physical and virtual, are available to all edge locations: physical and cloud datacenters, and branches.



Device clients

Establish the tunnel from a single device to the Cato PoP. The SASE client ensures traffic is encrypted, the tunnel is maintained as underlying networks change (moving between 4G/LTE, 5G and Wi-Fi), and the client-side implementation minimizes device resource utilization and power consumption.



The SASE Middle Mile: Global Private Backbone

The SASE global private backbone handles the traffic between the PoPs. There are two types of traffic to consider: northbound to the cloud and east-west between users and branches, and the enterprise datacenters.



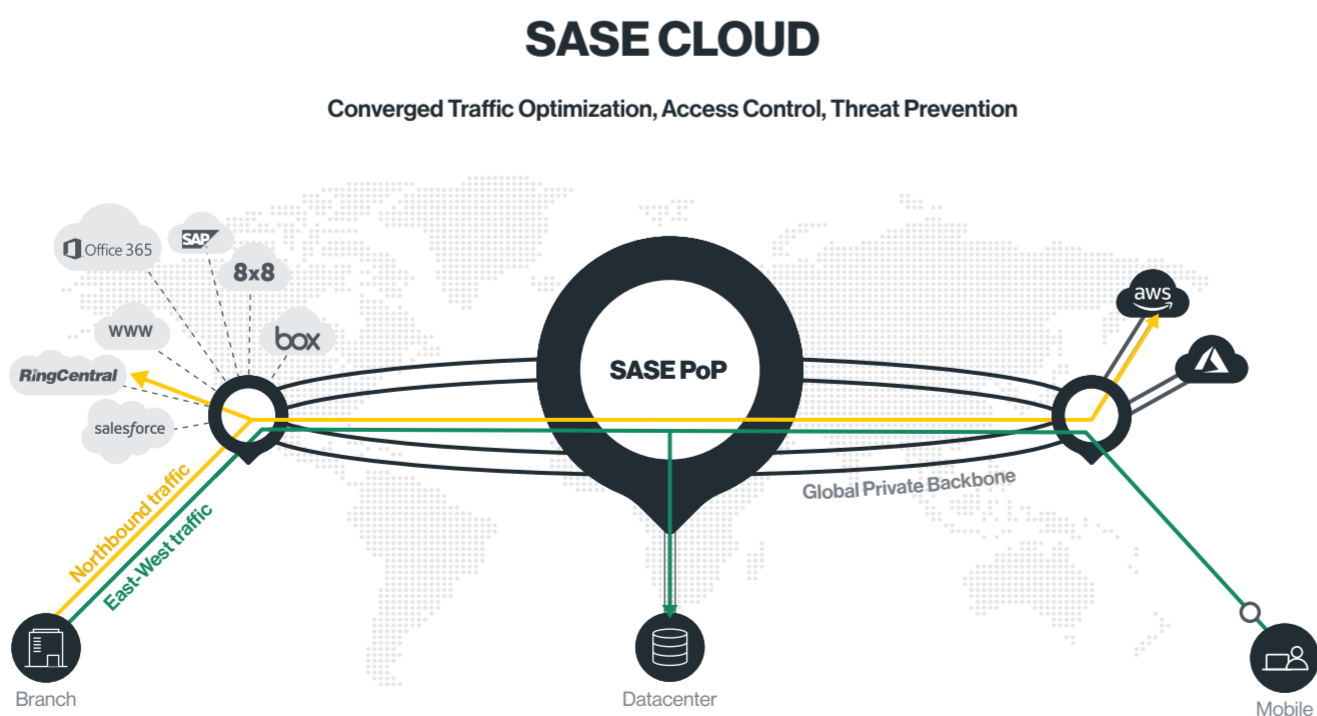
Northbound traffic

To optimize traffic to the cloud, a SASE global backbone should be co-located with primary cloud providers, linked with multiple Internet exchanges points shared with these providers, and in general, have sufficient density to maintain <5ms latency from key cloud destinations.



East-West traffic

To optimize WAN traffic between users, branches, and applications (often hosted in a physical datacenter), the SASE global backbone must be interconnected with tier-1 global carriers that overcome the unpredictable nature of the Internet. Critical traffic such as voice, video, remote desktops, and transactional business apps require optimal global routing, predictable latency, packet loss, and jitter, and network resiliency.



Capabilities: Security

SASE security capabilities **must** be delivered from the cloud. This is a non-negotiable requirement for a very simple reason: To deliver the same security capabilities to every location and user globally, without creating a very complex multi-tier network and security architecture, requires a single, global, and unified security architecture.

Below are listed the primary security capabilities that are within the scope of Gartner's SASE definition. Yet, unlike the architectural checklist above, the importance of these capabilities varies between enterprises, based on their specific priorities. Regardless, the convergence of these capabilities into a single pass engine, driven by a single policy is required to maximize efficiency and performance and reduce the risk of misconfiguration.



Firewall as a Service (FWaaS)

FWaaS enables customers to extend next generation firewall (NGFW) capabilities to locations and users without the need for a physical NGFW appliance on site. FWaaS enforces application-aware access control policy between sites and users and applies IPS policies on all traffic. Depending on the specific site requirements, it could control access between VLANs and subnets.



Secure Web Gateway (SWG)

SWG secures access to the Web. URL filtering and anti-malware is applied to the Internet traffic with full decryption and deep packet inspection. The cloud-based SWG eliminates the need for UTM appliances in the branch.



Cloud Access Service Broker (CASB)

CASB is used to discover cloud-based applications used in the business, understand how they are used and by whom, and control what kind of actions can be executed against them. CASB capabilities also extend to detect sensitive data types for compliance and can alert or block when such traffic or files attempt to leave the organization.



Zero Trust Network Access (ZTNA)

ZTNA provides a secure way for remote users and third-parties to access on-premises and cloud applications without granting full access to the network. Depending on the use case, cloud-based network access ("VPN") may still be required for some applications.

Requirement

While the capabilities above are described separately, a true SASE platform converges all of them into a single pass engine that applies one policy, across all security use cases, and for all traffic.

Capabilities: Management



One Console

SASE delivers a single pane of glass for accessing network analytics, security events, and policy configuration. Since the SASE management resides in the cloud, it leverages the cloud scalability, and massive storage capacity, to ensure fast response time and significant capacity for historical aggregation of data.



One Policy

A single SASE policy is more than a visual “stunt.” It is a key requirement for driving the single pass engine that is at the core of SASE. The SASE management system ensures that the full networking and security policy is valid and consistently distributed to all instances of the single pass engine throughout the cloud service. Regardless of which single pass engine serves enterprise edges, the enterprise policy is fully enforced at all times.



One API

SASE management APIs enable third parties (such as managed service providers (MSPs), to access or configure every object within the SASE data model. These includes, for example, the network performance metrics of a site over time, security events associated with a specific user, and the provisioning of a new location.

Requirement

A true SASE platform provides a single management application for all networking and security analytics and policy configurations. A single policy is deployed across all single pass engines within the cloud service to ensure consistent and continuous policy enforcement, and fast troubleshooting. A single API enables the automated access to SASE analytics and resource configuration for enterprise IT and service providers.

Checklist Table

1 Architecture

Attributes	Capability	Benefits
Converged	Secure and optimized network as a service, simple management and troubleshooting	Point solution elimination, cost reduction, grunt work relief
Cloud-based	Elastic, scalable, self-maintaining, self-healing, redundant cloud service	Simple capacity and availability planning (no scaling/sizing, built in HA)
Global	Available and extensible to every geography by design	Simple network design (no multi tier "hubs" and "colos")
All Edges	Extended to all edges: datacenters, branches, users, clouds, applications	Same enterprise capabilities to users everywhere (office, road, home)

2 Networking

On-Ramps	Capability	Benefits
SD-WAN	High performance and resilient location access to the SASE Service	Optimal and secure continuous network service (high uptime)
Remote Access	High performance and resilient user access to the SASE Service	Optimal and secure access for users from anywhere
Client	Support all applications, and all traffic for heavy users	Scalable full apps access (thick client, thin client, legacy, cloud)
Clientless	Support web-based application access for lightweight users and 3rd parties	Zero install optimal and secure access to modern web apps

Middle Mile	Capability	Benefits
Global Backbone	Predictable, redundant, backbone for WAN and cloud traffic	High performance global access to all apps
Northbound	Accelerates traffic to Internet and cloud destinations	High performance cloud apps access
East West	Accelerates traffic to WAN destinations (on-premises and in the cloud)	High performance WAN access to datacenter apps

3 Security

	Capability	Benefits
FWaaS	Access control between sites, segmentation	Firewall appliance elimination, No sizing/patching/upgrading
SWG	Threat prevention from Internet-borne attacks (phishing and malware)	Protect users from threats in the office, on the road, at home
CASB	Cloud apps and data visibility and access control	Control access to cloud apps and data
ZTNA	Secure and optimized remote access to users at home and on the road	Simple and secure remote access to all users everywhere

4 Management

	Capability	Benefits
One Console	A single interface to view and control all network analytics, security events, and policy configuration	Simple and easy network and security management, smart defaults out of the box
One Policy	A granular logical policy for the business enforced across the network	A network and security policy stated in business terms: locations, applications, groups, users.
One API	Programmatic Access and configuration of all systems objects	Deliver Cato raw data to SIEM, BI, and other reporting tools, allow MSP automated configuration at scale